SITE SECURITY FOR CHEMICAL PROCESS INDUSTRIES

A Thesis Submitted

In Partial Fulfillment of the Requirements
for the Degree of

Master of Technology

by

Shailendra Bajpai

to the

DEPARTMENT OF CHEMICAL ENGINEERING
INDIAN INSTITUTE OF TECHNOLOGY, KANPUR

JUNE, 2005

Certificate

This is to certify that the work contained in the thesis entitled "Site Security for Chemical Process Industries" has been carried out by **Mr. Shailendra Bajpai** under my supervision and that it has not been submitted elsewhere for a degree.

Date:

J P Gupta

Dr. J. P. Gupta

Professor

Department of Chemical Engineering

Indian Institute of Technology

Kanpur-208016

India

ABSTRACT

Chemical process industries such as oil refineries, fertiliser plants, petrochemical plants, etc., which handle hazardous chemicals, are potential targets for deliberate actions by terrorists, criminals and disgruntled employees. Security risks arising out of these threats are real and must be assessed to determine whether the security measures employed within the facility are adequate or need enhancement.

The essential components of security management programme include security risk assessment, security countermeasures, and emergency response. Security risk assessment can be carried out qualitatively by threat analysis, vulnerability analysis and developing Security Risk Factor Table. Threat analysis involves identifying types and sources of threats, and their likelihood; knowing adversaries, their intentions and capabilities. Vulnerability analysis identifies the weaknesses in a system that adversaries can exploit. Terrorists exploit the vulnerabilities to inflict maximum damage. They may find a target attractive based on the ease of attack and possible impact on facility. Depending on the threat likelihood and vulnerabilities, various security countermeasures are suggested to improve the plant security. Appropriate emergency response measures that could mitigate the consequences of a successful attack are also discussed. It is recognised that many of the conventional safety and security measures have to be modified in light of enhanced nature of threat. Two case studies: one of a fertiliser plant and the other on a refinery, have been performed to show the application of ideas presented.

ACKNOWLEDGEMENT

First and foremost, I would like to sincerely thank my thesis supervisor, Prof. J. P. Gupta for his invaluable guidance and encouragement throughout this work. The interest, which he has shown in this work, has boosted me a lot to perform well.

I am grateful to Dr. R. Sharma, Director, NIT Jalandhar for granting study leave and sponsoring my M. Tech Programme. I also wish to thank Quality Improvement Programme, MHRD, New Delhi for the financial assistance.

I am very grateful to all those, who have helped me immensely during my industrial visits and provided some very important information. I am thankful to Dr. G. N. Mathur for his discussion on perimeter fencing and security systems used in defence installations. I greatly appreciate the thoughts of Captain Umesh Chandra on general security issues.

I am indebted to my esteemed teachers for providing me the necessary academic background and help in every possible way at IIT Kanpur.

I thank my all colleagues, especially my lab mates Nitesh and Pramod, who made my stay at IIT Kanpur, memorable and pleasant.

I would like to express my deep respect to my parents, brothers and sisters who have always encouraged and supported me in whatever decisions I took. Finally, I would like to thank my wife, Vidushi for all the love and support.

Shailendra Bajpai

TABLE OF CONTENTS

List of Figures

List of Tables

Nomenclature

AACS	: Automatic access control systems
CCTV	: Closed-circuit television
CFC	: Chloro-fluorocarbon
COTS	: Commercial-off-the shelf
CPI	: Chemical process industries
ERP	: Emergency response plan
ERPG	: Emergency response planning guidelines
Hazchems	: Hazardous chemicals
HAZOP	: Hazards and operability analysis
ISP	: Inherently safer processes
LAN	: Local area network
MOC	: Management of change
MT	: Metric tonne
MTPD	: Metric tonne per day
PLC	: Programmable logic controllers
SRFT	: Security risk factor table
SVA	: Security vulnerability assessment
TA	: Threat analysis
VA	: Vulnerability analysis
VAM	: Vulnerability analysis methodology
WMD	: Weapon of mass destruction

Chapter 1

INTRODUCTION

Chemical process industries (CPI) are essential components of any economy, providing crucial support to manufacturing, agriculture and energy sectors, producing valuable exports and providing employment. However, these industries pose significant hazards to environment, workers and the surrounding community. The major extraordinary events that a chemical plant may experience in its life can be classified in three categories [1]:

1. Accidents that may occur due to technical failure or human error
2. Natural calamities such as tornado, earthquake, tsunami, etc.
3. Deliberate acts of sabotage by terrorists, disgruntled employees, etc.

1.1. A New Risk Paradigm

Prior to September 11, 2001, the risk assessment of CPI handling hazardous chemicals (Hazchems) was focussed on the analysis of risk related to unintentional acts such as accidents and natural calamities. Deliberate acts by terrorists or disgruntled employees, etc., were not included in the formal risk assessment. The events of 9/11 have changed the scene dramatically [2].

Chemical plants such as oil refineries, fertiliser plants, petrochemical plants, pharmaceuticals units, etc. that handle Hazchems are prime targets for terrorists and criminals. This is due to the fact that CPI store and transport bulk of the Hazchems, operate processes under extreme conditions of temperature and pressure, with fast material flows and complex kinetics. Terrorists having sufficient knowledge of the

chemical operations and layout of the plant may exploit these conditions, which may then lead to toxic release, fire and explosion further resulting in mass casualties, property damage, and economic and environmental impacts.

Therefore, the risks originating from deliberate acts are now considered both real and credible and must be examined to determine if the existing security measures are adequate or need enhancement. Security enhancements may be required, especially for the chemical sites that pose attractive target due to their economic importance, possible consequences, closeness to the population centres, etc. It is recognised that a facility itself can not prevent or protect against all suspected threats. However, these can implement reasonable security enhancements for high risks threats. A good co-ordination with local law enforcement agencies is required for sharing intelligence information, and managing emergencies [2, 3].

Innovative thinking is essential for dealing with intentional acts. Idea is to provide an element of surprise to the adversaries, prior to or during attacks. For example, change the protocol of storing Hazchems in storage tanks, or vary the routine being followed at the facility. Appropriate security countermeasures in place may help in hardening the target for adversaries. However, the chances of success for a determined adversary can not be ruled out. How to reduce the consequences in case of successful terrorist attacks is a challenging task. In fact, all conventional existing safety and security measures that are in place from years in CPI will still work for intentional acts as well, but many of these need to be significantly modified and supplemented by new ones. It is important to reduce the attractiveness of target in the eyes of adversaries [1].

The concepts of inherently safer processes may also prove to be quite useful in reducing the overall risk to CPI including those from deliberate acts. The essential elements for the site security of the CPI are:

- Security risk assessment
- Security countermeasures
- Mitigation and emergency response

1.2. Overview of Terrorism and Some Security Incidents

The terrorism is defined as, "the unlawful use of force or violence against persons or property to intimidate or coerce a government, the civilian population, or any segment thereof, in furtherance of political or social objectives [4]." It has become abundantly clear that various organizations and individuals are determined to use previously unseen means and forces to cause maximum damage and harm to governments, businesses, the environment, and the public. All sectors of economy are potentially subject to these illicit activities. The number of international terrorist incidents has increased in all parts of the world.

There have been several terrorist activities directed towards the CPI or their transportation systems so far. Further, the terrorists have demonstrated their capability in events of September 11 and the concern to protect CPI from intentional acts is further reinforced by the following incidents:

- In 1995, five members of a sect (Aum Shinrikyo) burst plastic bags filled with "Sarin gas" (nerve agent) on several lines of the Tokyo subway in an act of domestic terrorism. 12 people died and some 6000 were injured as a result of the attack [5].

- In 1997, four Ku Klux Klan members plotted to place an improvised explosive device on a hydrogen sulphide tank at refinery near Dallas, USA as a diversion for an armoured car robbery on the other side of the town [6].
- Anhydrous ammonia is a key ingredient in the illegal production of methamphetamine drugs. There have been numerous incidents worldwide where thieves, looking for ammonia for manufacturing illegal drugs, have broken into refrigerated warehouses, or ice manufacturing facilities, frequently leaving valves open. In some cases, the thieves have been overcome by the ammonia and needed to be rescued; in other cases, the community has been evacuated, and there have been injuries to the general public and to law enforcement personnel from exposures to the released ammonia [7].
- In 2001, the Trans Alaska pipeline in USA was closed for three days after it was hit by a bullet in the event described as drunken mischief. Over 6,000 barrel of oil was released [8].
- A cyber attack on a computerised waste-treatment system in Queensland, Australia, sent millions of gallons of raw sewage spilling into local parks and rivers. A 49-year old man, who worked for the supplier that installed the sewage system, angry over a job application rejection by the city, was found guilty of attacking the computerised system 46 times, and sent to prison for two years [6].

It is important to mention here that at present there is no legislation in any country that requires chemical plants to essentially conduct security risk assessment and maintain certain minimum security standard. However, in USA, two bills have been introduced to address chemical plant risks. New Jersey Senator Jon Corzine's "Chemical Security Act" is a serious set of requirements to improve safety and security at vulnerable facilities. The bill requires companies to implement inherent

safer technologies, wherever practicable and affordable. On the other hand, Oklahoma Senator James Inhofe's "Chemical Facilities Security Act" requires chemical facilities to complete vulnerability assessments and site security plans and imposes stiff penalties for companies that fail to comply with the law [9].

1.3. Security Risk Management

Security risk management programme requires a systematic approach to analyse security risks [10]. The process involves identifying critical assets to be protected, identifying credible threats from various adversaries, assessing vulnerabilities and risks, and evaluating the adequacy of countermeasures (Figure 1.3.1). The analytical part of this process is called Security Vulnerability Assessment (SVA). SVAs are not necessarily a quantitative risk assessment, but are usually performed qualitatively using the best judgement of the SVA Team. The expected outcome is a qualitative determination of risk to provide a sound basis for rank ordering of the security-related risks and thus establishing priorities for the application of countermeasures. Different organisations have developed their own SVAs that are best suited for them [4, 11, 12].

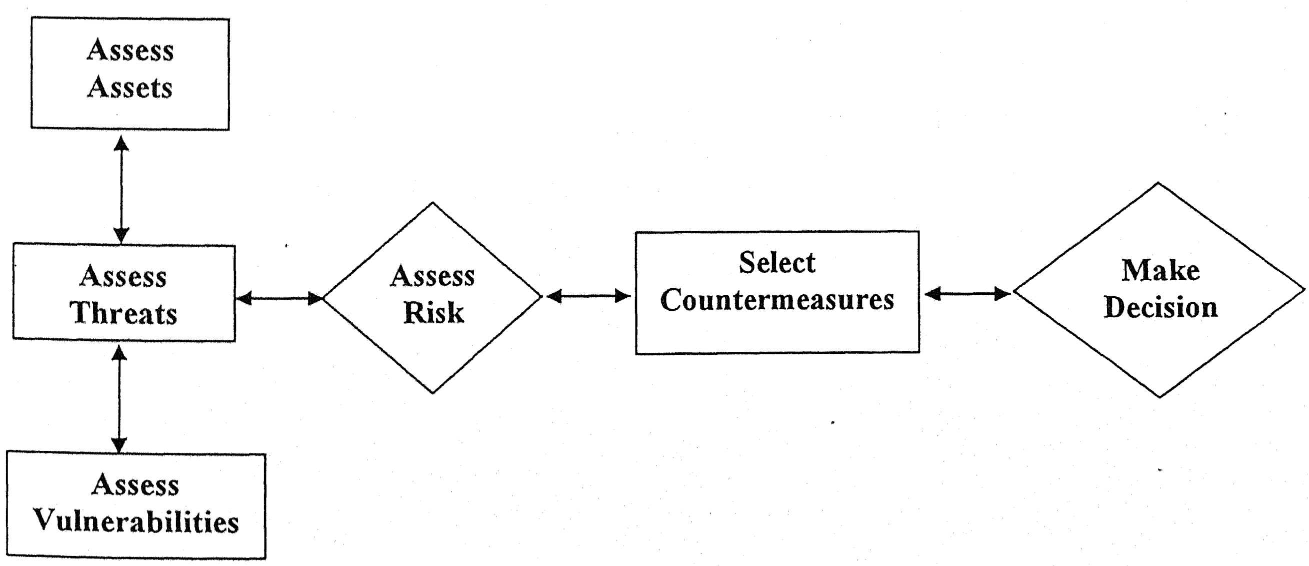


Figure 1.3.1. Security Risk Management Process [10]

It is the responsibility of the owner/operator to choose the SVA method and depth of analysis that best meets the needs of the specific location. Differences in geographic location, type of operations, and on-site quantities of Hazchems all play an important role in determining the level of SVA and the approach taken. Independent of the SVA method used, all techniques include the following activities [4, 12]:

- **Asset Characterisation**: Characterise the facility to understand what critical assets need to be secured, their importance and their interdependencies and supporting infrastructure.
- **Threat Assessment:** Identify and characterise threats against those assets and evaluate the assets in terms of attractiveness of the targets to each adversary and the consequences if they are damaged or stolen.
- **Vulnerability Assessment**: Identify potential security vulnerabilities that threaten the asset's service or integrity.
- **Assessment of Security Risks**: Determine the risk represented by these events or conditions by determining the likelihood of a successful event and the consequences of an event if it were to occur. Rank the risk of the event occurring and, if high risk, make recommendations for lowering the risk.
- **Recommendations:** Identify and evaluate risk mitigation options (both net risk reduction and cost benefit analysis) and re-assess risk to ensure adequate countermeasures are being applied.

1.4. OBJECTIVES

The main aim of the present work is to assess the security risks of CPI and their transportation systems from deliberate acts and recommend appropriate security enhancements. There are two essential aspects that need attention. First, how to reduce the target attractiveness of the facility in the eyes of adversaries. And second, what should be done to reduce the consequences in case of successful attack.

Chapter 2

LITERATURE REVIEW

Prior to 9/11 events, risk management of CPI was focussed on accidental releases and it excluded most considerations on intentional releases. After the September 11, 2001 the scene has changed dramatically and there is a real concern as well as a sense of urgency for protection against deliberate acts in CPI.

The American Chemistry Council (ACC), the Chlorine Institute, and the Synthetic Organic Chemical Manufacturers Association (SOCMA) [11] jointly developed and issued 'Site Security Guidelines for the US Chemical Industry' in October 2001. The American Petroleum Institute (API) [4] published similar guidelines for the petroleum industry in April 2003.

In the year 2002 and 2003, several other Security Vulnerability Assessment (SVA) methodologies were developed by various organisations such as:

- The American Institute of Chemical Engineers (AIChE)/Center for Chemical Process Safety (CCPS) [12] published 'Guidelines for Managing and Analyzing the Security Vulnerabilities of Fixed Chemical Sites', August 2002.
- Synthetic Organic Chemical Manufacturers Association [13] published 'SOCMA Manual on Chemical Site Security Vulnerability Analysis Methodology and Model', November 2002.
- American Petroleum Institute (API)/National Petrochemical and Refiner's Association (NPRA) [14] published 'Security Vulnerability Assessment Methodology for the Petroleum and Petrochemical Industries', May 2003.

Each of the methodologies mentioned above employs traditional risk assessment techniques and provides a well-defined, systematic framework to identify security threats, risks, and vulnerabilities.

There are several published articles in the field of process security that extend the work published in the above SVA methodologies.

Baybutt [15] has mentioned the importance of risk assessment for process security management. He mentioned the importance of developing a threat profile by analysing motivations and capabilities of adversaries and rating of security facility factors. He performed risk assessment by conducting threat and vulnerability analyses.

He [6] proposed a comprehensive programme for process security management that parallels process safety management, which address accidental releases of Hazchems. He outlined the overall process security management process and described its difference with process safety management.

He [16] also pointed out the application of inherent security and safety approaches that could reduce the likelihood and severity of a successful attack. According to him, this could be the first layer of defense.

Lemley et al. [17] categorised threats, target vulnerabilities and consequences in a single summary matrix. They studied the intentions and capabilities of different adversaries and how these relate to profiling risks for different locations of a plant.

Jaeger [18] developed a vulnerability assessment methodology (VAM), which is a systematic risk-based approach where risk is a function of the severity of consequences of an undesired event, the attack potential, and the likelihood of adversary success in causing the undesired event. VAM consisted of 13 steps: Screening, vulnerability assessment project definition, characterisation of facility,

derivation of consequence severity levels, threat assessment, identification of priority cases for analyses, preparation for analyses, site survey, system effectiveness analyses, risk determination, recommendations for reduction of risk, consideration of impacts and final report preparation.

Moore [19] explained the importance of a new risk management paradigm for chemical plant security that would require a different form of analysis than accidental risk assessment methods. He overviewed the concepts of SVA and security management principle. He explained that deliberate release risk could be managed by many of the same or similar strategies as accidental release risk. According to him, traditional security countermeasures, such as physical security features and cyber security measures, must integrate with safety strategies to result in a single process risk management strategy.

Stickles et al. [20] discussed the importance of SVA and summarised the features of three popular SVA methodologies from ACC, CCPS and Sandia Laboratory. They presented a case study that illustrated how hazard modelling can assist in quantification of the impacts of threats and the development of mitigation concepts. In this case study, they considered the following scenario:

A terrorist loads an explosive on the back of a truck, and parks the vehicle in close proximity to a storage tank containing a toxic chemical. The vehicle is parked on the side of the road outside the plant fence line. The storage tank is located about 61 m from the road. For illustrative purpose, they assumed that the vehicle contains the equivalent of about 544 kg of TNT. They showed that the resulting overpressure would cause the storage tank to rupture. This would result in a toxic release, which would go a distance of 8 km to the ERPG-2 level of concern. Therefore, they

concluded that the scenario has a severe off-site impact, and the security requirements for mitigating this scenario need to be explored in greater detail.

Coster et al. [21] analysed the vulnerability of CPI to terrorist attack and identified nine factors (access, security, visibility, opacity, secondary hazard, robustness, law enforcement response, victim profile, and political value) that might be used as a starting point for a more formal risk assessment. They realised that an important aspect of risk assessment peculiar to antagonistic hazard and terrorism was the distortion of the usual frequency–severity curve in which high mortality events were generally less likely than low mortality events

Emerson et al. [22] examined security issues from the unique perspective of nation's coastlines and associated infrastructure. They emphasised the ongoing efforts to secure offshore shipping lanes, as well as the transportation systems. They showed for the coast guards, layered defense could be broken down into four zones: foreign ports, offshore, coastal, and dockside.

Ragan et al. [23] pointed out the need of modifying plant's existing safety plan for the acts of terrorism and sabotage. They studied some terrorist proof measures (use of excess flow valves, reaction inhibition systems, trained emergency response teams, etc.) that were being placed in chemical plants for many years. They also suggested some site security related actions, such as improving fences and lighting in plant, adding remote cameras where regular patrol is not practicable, and having good co-ordination with local law enforcement agencies, etc., that a plant could incorporate. They showed that specific scenarios could be analysed by using causal-tree method. They developed a causal tree for the inadvertent/deliberate addition of a contaminant to a tank containing reactive chemicals. They showed that by constructing such diagram, weaknesses in the protection of tank from terrorist or

sabotage attack could be identified and relevant security enhancement can be suggested. They considered secrecy as an important layer of protection and identified some additional hazards presented by terrorism and sabotage.

Whiteley et al. [24] studied the level of safety provided by existing plant equipment and safety systems in response to a terrorist attack. They suggested to consider the terrorist or criminal threat from a process, rather than security, point of view. They explained that all process plants are designed to deal with unintentional events such as equipment failure, loss of utilities, fire exposure from spills, etc. that threaten safe operation of the facility. However, existing safety systems were not designed to address acts of sabotage or a thinking adversary. They suggested integrating the results of SVA and HAZOP to automatically produce threat scenarios. They emphasised on the utility of mapping inventories of Hazchems in the process in terms of explosive energy or fire. They concluded that work is required to:

(1) Determine how existing Process Hazard Analysis (PHA) methods could be modified to address the threat of terrorist acts, and;

(2) Determine what changes in equipment, policy, and procedures could be implemented to minimise the impact of a terrorist attack (process threat management).

Teumim [25] showed the vulnerability of Supervisory Control and Data Acquisition (SCADA) systems connected directly to business networks of their companies and especially the internet. He further explained the emerging threats of conventional and cyber terrorism with the help of a hypothetical scenario. He considered a 60 cm diameter buried, high pressure (8,273 kPa) natural gas transmission pipeline crossing under a two-lane highway leading to a small town. A disgruntled employee, who was working in a nearby compression station, exploited

the vulnerability of NT working station attached to company's Local Area Network (LAN) and modified the Programmable Logic Controllers (PLC) to disable the remote operated shut-off valve. He further, with the help of a grenade, made an explosion near pipeline in order to disrupt the gas supply. However, he got killed in the resulting fireball and a major release was caused. The emergency responders could not isolate the ruptured section as the disgruntled employee previously disabled the remote operated shut-off valve.

In the next Chapter, various security risk assessment techniques are discussed.

Chapter 3

SECURITY RISK ASSESSMENT

Security risk assessment can be been carried out qualitatively by following:

- Threat analysis
- Vulnerability analysis
- Security Risk Factor Table

3.1. Threat Analysis

Threat analysis (TA) is used to identify the sources, types of threats, and their likelihood. It involves study of all issues that are critical to the likelihood of threat such as history of security incidents in and around the facility, intentions and motivations of adversaries, their capabilities, etc. It is important to mention here that even a small security incident like theft of confidential information may be a precursor to the planned terrorist attacks [2, 3].

The attack is normally well planned, and it may take years for terrorists to gather important information about the site and look for vulnerabilities. They may also involve some insiders either by luring them for great monetary reward, or by threatening them of dire consequences. The main focus is on the terrorist attacks that might result in a large release of Hazchems, major explosion or fire, further resulting in disruption of business activity, casualty, economic loss, etc. [2]. The aim of this exercise is to identify the specific threats that are credible to the location of the given plant.

Type of threats: The following list includes some of the potential threats to a chemical plant due to deliberate actions by terrorists or other adversaries [2, 4, 12]:

- Release of Hazchems on-site causing fire, explosion, and toxic gas dispersion
- Theft of Hazchems for utilising off-site
- Complete shut down of the plant
- Major damage to the plant infrastructure
- Product tampering
- Theft of confidential information
- Vandalism of control rooms and equipment
- Bomb threats
- Creation of destructive situations through tampering with valves, etc.
- Cyber attack to disrupt computer controlled equipment
- Disabling security systems
- Sabotage not considered above such as incapacitating plant operators, security guards, etc.

Sources of threat: They can be broadly divided into 2 categories: internal threats and external threats (Table 3.1.1). Internal threats come from disgruntled employees, former employees, visitors, or anyone having routine access to the plant. Insiders pose a particular difficult threat due to possibility of deception, knowledge about the facility and unsupervised access to the critical assets [17].

Table 3.1.1. Sources of Threats

S. No.	Internal Threats	External Threats
1	Disgruntled or former employees	International terrorist groups
2	Contractors or suppliers	Regional terrorist groups
3	Visitors and customers	Psychotics
4	Vendors	Vandals/Cults
5	Any other person having a routine access to the plant	Hackers
6		Violent activists

External threats principally come from terrorists, saboteurs, hackers, hostile foreign governments, criminals, cults, etc. Different adversaries have different motivations, intentions and capabilities. For example, a disgruntled employee may have lost faith in the company and may want to take revenge by disrupting the production. His basic intention is to cause economic damage rather than inflicting injuries to people [19, 26].

However, the major threat to the CPI is from external adversaries such as terrorists, criminals, cults, etc. having clear intention to inflict a large number of casualties. Terrorists may commit such acts for political, religious, economic, social or some ideological reasons. They are even ready to die for the success of their mission. They are highly trained, motivated and intelligent people with an intention to draw the attention of public, media, and government towards them by creating terror in the society. They find unique ways to attack and try to exploit energy already present at the location. For example, they may use a truck tanker carrying flammable

material as a mobile explosive device. Terrorists frequently use conventional bombs, military explosives, automatic rifles, rocket launchers, etc. The most serious threat is posed when knowledge of an insider is coupled with the capabilities of external adversaries [3, 20].

The domestic terrorist groups, violent activists, etc. have shown many activities in the recent past, so a CPI situated in those regions must include the specific threat from these groups. On the other hand, the threat from international terrorist groups must be included in threat analysis at all places [2].

The important information to be included in TA is as follows [2, 4, 15]:

- Mention all sources of threats (deliberate action by terrorists, disgruntled employees, criminals and others)
- State capability, motivation and impact of different adversaries
- List the Hazchems being used in the facility
- Identify the locations where the Hazchems are stored and processed (mention the quantity stored or processed)
- State proximity of Hazchems from plant boundary
- List the presence of chemicals that can be used as or precursor to the weapon of mass destruction (WMD) such as chlorine, phosgene, nerve agents, etc.
- Obtain the history of safety and security incidents in and around the facility
- State existing security measures being employed at the facility
- List weaknesses in the existing security
- Mention facility location: rural, urban, or close to high population density
- Mention importance of the product
- State facility visibility from roads, or rail
- State ownership of the facility: private, public or government installation

The risk posed by a given threat depends on various factors that account for its severity & likelihood (Figure 3.1.1). There are various factors that contribute to the likelihood of a threat such as target attractiveness factors, severity of attack, and ease of attack. Target attractiveness factor includes location of the facility, visibility, ownership, importance of the product to the economy, etc. Severity of attack includes inventory size, presence of Hazchems in facility, and proximity to the populated area, etc. Ease of attack includes in-effectiveness of security countermeasures, gaps in the security, ease of access to the critical area, etc [3].

It is important to think ways of making CPI a less attractive target for terrorists. For example, avoid signage on storage tanks or road tankers carrying hazardous chemicals. Brainstorming is required to reduce the severity of consequences in case of a successful attack and make these facilities a difficult target for terrorists attack.

SEVERITY	Moderate risk	High risk	Very high risk
	Low risk	Moderate risk	High risk
	Very low risk	Low risk	Moderate risk

LIKELIHOOD

Figure 3.1.1. Risk Assessment Matrix

Security related incidents in and around the facility must be properly investigated and documented, since these incidents may be an indication of a well-planned terrorist attack. Some of the security related incidents that need attention include [14]:

- Cases of theft/violence
- Dilapidated fence
- Occurrence of unauthorised entry of vehicles, employees, etc., in restricted areas
- Unknown person taking photograph of the site
- Major unexplained process upset
- Abrupt loss of containment of Hazchems

TA as discussed here is a qualitative risk assessment. It is a snapshot in time; therefore it must be updated at least annually depending on the threat environment and given circumstances. Threat related information should be obtained from local law enforcement or intelligence agencies. It is important to have close association with them [2].

3.2. Vulnerability Analysis

Vulnerability analysis (VA) is used to assess the degree to which a facility is susceptible to hostile action from the adversaries. It involves identifying ways in which the credible threats identified in threat analysis could be realised [2]. The analysis is accomplished by dividing the plant into several zones, associating with these zones certain credible threats and identifying their respective vulnerabilities. Since terrorists employ novel ways to strike, so it is essential to be creative and imaginative in VA.

The team that conducts VA must have professionals from the field of safety, security, maintenance, management, facility engineer, instrumentation engineer, computer expert, human resource, local law enforcement officials, etc. Help can be sought from some intelligence agencies as well. The team gathers the relevant information, surveys the site and surrounding areas, conducts interviews, and assesses the threats, vulnerabilities and consequences, etc. Idea is to look for the vulnerabilities in the facility that can be exploited by the adversaries. The best thing is to think like adversaries. Assume that the given chemical plant is a target, and members of the team are adversaries. It is important to think what all can contribute in making a plan and what are the resources present in the environment that can be exploited to enhance the impact. What could be the possible scenarios, in which adversaries can attack, has to be identified and analysed further. Brainstorming is required and innovative thinking is a must in developing scenarios. Some of the important questions that need to be answered while conducting VA are:

- What are the assets that need to be secured?
- What information is critical and sensitive?
- What are the credible threats?
- Who are the adversaries?
- What are the vulnerabilities?
- Are there any security-gaps?
- What are the likely scenarios in which threats could be realised?
- What are the common tactics and capabilities of possible adversaries?
- What security upgrades are required to fix vulnerabilities and to harden the target?
- What are the worst possible consequences in case of successful attacks?

It is possible that some scenarios may be missed out in VA. Idea is to find out the most likely scenarios in which a particular threat may be realised.

VA is carried out through the following steps (Figure 3.2.1) [2, 13, 15, 18]:

- Divide the plant in to different zones of security to lend focus to the analysis. It is important to identify the critical assets in the plant, for example, storage tanks containing Hazchems or equipment operating under extreme conditions of temperature and pressure.
- Identify the threats from potential adversaries in each zone, for example toxic release by terrorists or disgruntled employees in a tank farm area. All credible threats as already identified by TA have to be considered in VA.
- Identify the vulnerabilities within each zone. Develop various scenarios in which the credible threats identified in TA could be realised.
- State worst possible consequences in case of a successful attack.
- Assess security risks by evaluating severity of consequences and likelihood of successful attack.
- Recommend additional security measures to be adopted in light of the nature of threats, process vulnerabilities, possible consequences and existing security measures.

Sample vulnerability assessment worksheet can be completed for a specific asset detailing its threats, vulnerabilities, consequences and recommendations (Table 3.2.1). It is important to perform cost benefit analysis before implementing new security measures.

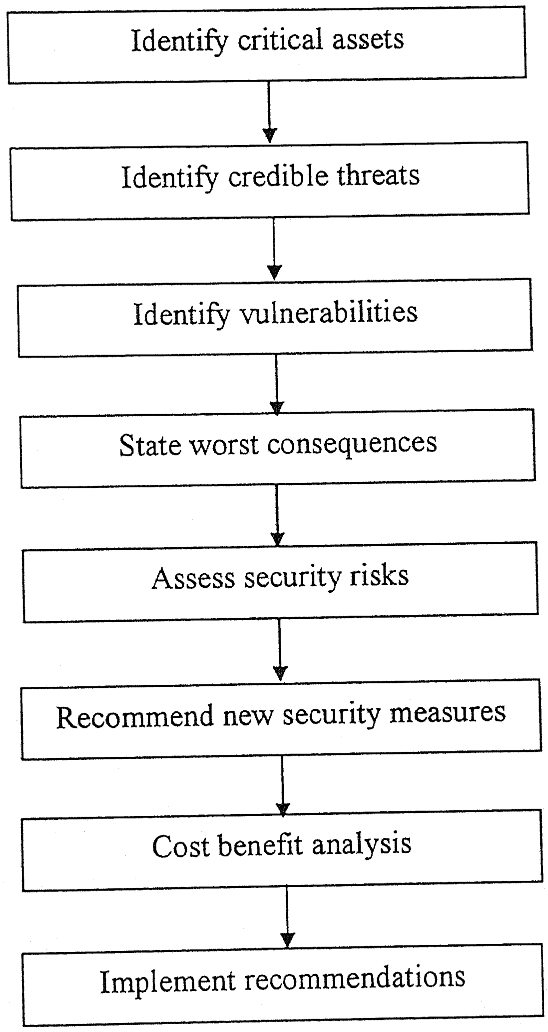


Figure 3.2.1. Flow Chart of Threat and Vulnerability Analysis

Table 3.2.1. Sample Vulnerability Assessment Work Sheet for CPI [15]

Threats	Vulnerabilities	Consequences	Recommendations
Hazardous (flammable and/or toxic) substance release caused by terrorists from outside boundary.	1. Storage tanks are visible from road, labelled and are situated close to perimeter. 2. Plant is located near high population area or close to some important government establishment. 3. Plant boundary is damaged. 4. No guard patrol in critical areas during daytime. 5. Projectiles could be fired.	Mass casualties both on- and off-site, environmental contamination, financial loss and damage to company image.	1. Store less amount of Hazchems in tanks that are close to perimeter and avoid signage on it. 2. Improve perimeter fencing with electronic surveillance and install proper area lighting. Install CCTV monitoring where regular patrol is not feasible. 3. Consider around the clock guard patrol for all critical areas. 4. Consider implementing blast resistant designs for equipment handling Hazchems.

Contd...

Table 3.2.1. Sample Vulnerability Assessment Work Sheet for CPI (Contd...)

Threats	Vulnerabilities	Consequences	Recommendations
Hazardous (flammable and/or toxic) substance release caused by disgruntled employee from within.	1. Employee access to critical area is not controlled. 2. Drain valve can be opened manually. 3. Control system may be disturbed. 4. Poor labour relation in the plant. 5. No policy to conduct background checks on employees.	Casualties on-site, financial loss, environmental contamination, loss of confidence in employees and damage to company image.	1. Restrict access of employees to the critical areas. 2. Consider installing valve locks. 3. Restrict access to control system with password control. 4. Maintain good labour relation in the plant. 5. Conduct background checks on employees.

3.3. Security Risk Factor Table

The current security risk status of a facility can be assessed by developing a Security Risk Factor Table (SRFT). In SRFT, all risk factors that influence the overall security of the plant are identified and rated on a scale from 0 to 5, with 0 being the "lowest risk" and 5 the "extreme" [27]. The total score obtained from SRFT helps in assessing the current security risk status of the facility (Tables 3.3.1 and 3.3.2). For a given facility, SRFT can be used as pre-screening tool to know whether a detailed threat and vulnerability analysis is required or not.

Table 3.3.1. Security Risk Factor Table [27]

Risk factors	**Range of security points**				**Actual points**
Location	Rural 1	Urban 2,3,4		High density 5	
Visibility	Not visible 0	Low 1,2	Medium 3,4	High 5	
Inventory	Low 1	Medium 2	Large 3,4	Very large 5	
Ownership	Private 1	Public/Co-operative 2,3		Government 4,5	
Presence of chemicals which can be used as precursors for WMD	Absence 0			Presence 5	
Worst case impact on-site	Negligible 0	Low 1	Moderate 2,3,4	Severe 5	
Worst case impact off-site	Negligible 0	Low 1	Moderate 2,3,4	Severe 5	

Contd…

Table 3.3.1. Security Risk Factor Table (Contd...)

Risk factors	**Range of security points**			**Actual points**
History of security incidents	Nil 0	Few 1,2,3	Frequent 4,5	
Presence of terrorist groups in region	Absence 0	Few 1,2,3	Large no. 4,5	
Existing security measures:	High level	Ordinary	Poor / None	
• Access control	1	2,3	4,5	
• Perimeter protection	1	2,3	4,5	
• Mitigation potential	1	2,3	4,5	
• Proper lighting (all over)	1	2,3	4,5	
• Use of Metal detector/ x-ray/ CCTV (at entrance and at all critical locations)	1	2,3	4,5	
Personal preparedness and training	Well prepared 1	Average 2,3	Poor 4,5	
				Total score =

Table 3.3.2. Security Risk Rankings [27]
(Based on score obtained from SRFT)

Current security risk status	**Actual points obtained**	**Recommendations**
Low	<15	Maintain security awareness without excessive concern.
Moderate	16-30	Review and update existing security procedures in light of possible threats.
High	31-45	Identify risk-drivers that can be reduced with reasonable controls. Conduct threat & vulnerability analysis and work with law enforcement agencies to enhance security.
Extreme	>45	Initiate aggressive risk-reduction activity, in conjunction with consultation with law enforcement agencies. Conduct threat and vulnerability analysis.

Chapter 4

SECURITY COUNTERMEASURES AND RISK MANAGEMENT

This chapter describes what can be done to enhance the security of CPI to combat terrorism. Conducting security risk assessment helps in identifying the appropriate security countermeasures and risk management strategies for a given facility. Traditional security management involves four key steps to intercept and neutralise a threat scenario [22]:

1. Detect
2. Delay
3. Respond
4. Mitigate.

- Detection is the ability to discover and identify when an attack occurs. It includes alarms, intrusion detection systems, parcel screening, cameras and sensors.
- Delay of attack requires deterrence of adversaries before they accomplish their goals. It includes physical barriers for personnel entry and vehicles, ringing assets with fence, proper area lighting and information security.
- Response requires a timely intervention between adversaries and assets to thwart the attack. It includes restricting access to critical areas by employees, contractors, etc., and emergency shutdown during attack.
- Mitigation requires effective procedures to neutralise the impact of threat. It includes stockpiling chemical antidotes, engineered process safeguards, blast

resistant structures, emergency response and communication with local law enforcement personnel.

4.1. Security Countermeasures

Security countermeasures are the steps that can be taken to strengthen the weak points in a system, either by lessening vulnerabilities or by hardening the facilities. These can be classified in the following categories:

- Information security
- Cyber security
- Physical security
- Policies and procedures
- Training

4.1.1. Information Security

Security of a site depends on the amount of information available openly about its layout, process conditions, recipe, inventory of Hazchems and existing security measures. The first step towards security is thus protected and limited access to sensitive information. The success of a terrorist attack would greatly rely on the extent of correct information available with them. Information should be protected in all its forms, whether written, electronic or spoken. CPI management must be careful with [2, 6, 12]:

- Information available on internet, intranet and media about the company.
- Information revealed in weekly bulletins, magazines, newsletters and annual reports.
- Sensitive information being inadvertently revealed.

4.1.2. Cyber Security

CPI extensively use computers for various activities such as control systems, emergency response systems, access control, power, transportation, communications, etc. These computer systems are vulnerable to cyber attack from external adversaries as well as ill-willed insiders. The adversaries can harm the facility in numerous ways, leading to loss of critical information, business interruption, toxic release, etc. Some important points to consider include [2, 25, 28]:

- Provide adequate physical security and control access to the computer rooms, server rooms, telecommunication room, rack rooms, etc. Use biometric authentication in these places.
- Protect computer network with firewall, encryption, password control, antivirus software, etc.
- Do not allow access to the process control system from remote computers.
- Do not post signs indicating the location of the computing facility.
- Provide reliable communication facilities to control room to facilitate prompt reporting of emergencies.
- Internet and the intranet are the common sources of insider or outsider hack attacks. Computers attached to the critical systems may be de-linked from corporate network, local area network (LAN) and internet thus allowing no network cross connections. If quick flow of information to business databases and management is required, then a partial measure would be to place an internal firewall that only allows certain restricted traffic between the business and process control networks.
- Do not allow commercial-off-the shelf (COTS) software such as e-mails, web browsers, etc., to run on computers attached to critical control systems.

- Train employees for making strong passwords, and not sharing it with others. Passwords should be changed periodically.
- Regularly patch-up the vulnerabilities present in the system, by updating the system, with latest patch available in the market.
- Maintain regular back-up of critical data.
- Provide power back-up for all computer controlled operations.

4.1.3. Physical Security

Physical security (PS) deals with the prevention or control of access to a facility. It makes the target difficult and reduces the likelihood of a terrorist attack. The following PS measures may be incorporated to enhance the security of CPI:

4.1.3.1. Perimeter Protection

Physical barriers, lighting, guard posts and patrols; supplemented by the alarm system, CCTV and other electronic devices serve to detect and deter would be intruders. Fences, block walls, building perimeter walls and structural barriers commonly form the basis of perimeter protection. The determined adversaries can penetrate almost any barrier, but the barriers act as a delaying factor and also are a psychological deterrent [29, 30].

Perimeter Fencing

It is important to fence the site appropriately. Consider fencing key areas and critical assets. Fencing used as a perimeter barrier must be at least 182 cm in height, plus a 30 cm top guard of barbed wire, with the angle arm facing out. In the case where a building facade is part of the perimeter, provide appropriate locking devices for all windows and doors. Consider placing the perimeter under supervision using

intrusion detection technology (sensor alarms), video surveillance, or both. Clear zones should be maintained on both sides of the fence. Shrubbery and weeds that could provide cover for an intruder should be cut away. Pay particular attention to the neighbouring structures, trees, utility poles, etc. that may help intruder to cross the perimeter. Openings in any perimeters should be kept to the minimum and all of these should be guarded and secured properly. Gates and doors not in use should be locked [2, 29].

Alarm perimeter protection

Various types of sensors are available in the market that are designed to detect the presence of an intruder in an area. Following are amongst the most popular systems used for alarming perimeter [29, 31]:

- ***Fence disturbance sensors*** are designed to discriminate between the higher frequency vibration caused by intruder and lower frequency vibration caused by wind.
- ***Microwave and infrared systems*** send an invisible beam of infrared/microwave energy from a transmitter to a receiver and detect the intruder moving through the beam.
- ***Buried pressure sensors*** detect the pressure of an intruder passing over a buried cable.
- ***Electrostatic fences*** utilise an electric field generated along a series of wire that comprise a fence. When an intruder's body changes the electrical field level to a certain degree, an alarm is activated.
- ***Ultrasonic systems*** emit patterns of radio frequency waves, and alarm when the signals are altered by the presence of an intruder.

4.1.3.2. Lighting

Inadequate lighting poses a major vulnerability that can be exploited by the adversaries. Proper illumination, all over the site, should be provided to permit detection and assessment of adversaries. It also helps to reveal unauthorised persons, and permit examination of credentials and vehicles at pedestrian and vehicle entrances. Security and safeguard lighting systems used for illumination should have a backup electrical power system. There should be minimum of shadows and the intention should be to direct the glare of light into the eyes of adversaries while eliminating glare for the protective force. Lighting fixtures should be positioned to produce overlapping beams of light; thus a burned-out lamp does not leave an area of total darkness. Lights should be placed high enough and enclosed in a vandal-proof housing to eliminate the possibility of tampering or damage [29, 30].

4.1.3.3. Closed-Circuit Television (CCTV)

Install CCTV at main entrance, near critical locations, and areas where regular patrol is not feasible. The cameras should be equipped with pan, tilt and zoom features and can be monitored from control room or guard room. The cameras should be placed high and in housings that are resistant to both weather and tampering [2, 30].

4.1.3.4. Protective Force

It is very important to have well trained and adequately equipped security guards for CPI. They should be physically fit and aware of safety and emergency procedures of a facility. Exterior guard patrols should be established on an hourly basis but should not conform to any set time pattern. CPI are normally large facilities,

so these must have a few patrol vehicles equipped with two-way radio and spotlight. Guard dogs can also be considered for facilities where exterior grounds are extensive [1, 30].

4.1.3.5. Guard Towers

It is possible to monitor the activities on both sides of the perimeter from a guard tower. Therefore, these should be positioned all around the perimeter such that there is no dead spot and are designed to withstand blast and weather extremities. Ensure around the clock surveillance from guard towers in critical locations. These should be equipped with [3]:

- Secure communication to central security room
- Assault rifle, night goggles and telescope
- Alarm system to alert security control room
- Back-up person to relieve guard in an emergency

4.1.3.6. Anti Vehicle Barriers

Permanent metal pipe or concrete barriers should be placed around critical above ground structures, robust enough to stop or deflect assault by a speeding vehicle. Since terrorists frequently use vehicles as a mobile explosive device, vehicle barriers should be provided near all critical places in a facility [30].

4.1.3.7. ID Badges

All employees and contractors should be issued regular site access photo ID badges, which should be displayed while personnel are on site. All visitors (including

non-regular employees) should be required to sign in and present positive picture identification before being granted access to the facility [29, 30].

4.1.3.8. Automatic Access Control Systems (AACS)

Procedural access control is often supplemented by the AACS. There are times, when it is not feasible to have security guards or a receptionist to admit the individual to the building or some secured area within the building. At such times various electronic and magnetic devices can be employed to control access. Smaller companies may also use them for reducing security manpower. Some important AACS include [29, 30, 31]:

- ***Magnetic card entry*** can be installed in any gate, and especially for parking lot gates. The system utilises a plastic card that has series of mini-magnets embedded within the plastic at one of the edges. Some other card systems are coded using computer chip technology.
- ***In digital systems,*** the locking device is operated by a combination, which must be correctly pressed for opening the door. The unit can be programmed to sound an alarm, when improper combination is pushed. It is important to change the combinations at regular intervals, especially when a key employee is terminated or transferred to other location.
- ***Key lock entry identification systems*** are often installed where management wants to know who entered and when. It has a locking system which records on a pressure sensitive tape the key that was used to enter and the exact time the entry was made. This system can be used in file rooms, vault areas and areas containing sensitive information, etc.

- ***Biometric authentication systems*** verify the persons by means of personal characteristics such as face, retinal pattern, signature, gait, hand geometry, voice, etc. Biometric systems should be used in control rooms and other high security places.

4.1.3.9. Other PS measures

- Examine persons and parcels with explosive and metal detectors.
- Ensure X-ray screening for closed packages.
- Ensure proper communication in the plant: radio, intercom, telephones and public address system.
- Avoid marking on tanks containing Hazchems.
- Consider using 'jammers' that will jam the frequency of operation of a remote controlled explosive device. They can be placed near critical locations.
- Consider installing wireless sensors on the equipment to measure variables like temperature, pressure, volume, level, etc. This will reduce the vulnerability of long wires, which can be cut by the adversaries.

4.1.4. Policies and Procedures

Policies state the management's position and philosophy on key issues while procedures define the most appropriate way of performing a task. Some important procedural countermeasures a chemical facility should implement include [2, 12, 23]:

- Background check of all employees should be done through appropriate agencies before hiring and periodically thereafter, say every five years. Be alert to any sudden happenings in their family: major medical expenses, loss of near ones, becoming more religious minded, purchase of very expensive homes or holidays,

etc. and see if their behaviour changes. Employees' entry in critical locations should be restricted.

- Visitors should be admitted to the site for a genuine purpose only. They should not be allowed to visit the restricted areas, unless approved by the management. All visitors should wear badges that are distinct from the employee and contractor ID badges during their stay on site. All group visitors should be escorted and the escort should remain with the group for the entire visit.
- All contractors and temporary personnel must be screened in accordance with company policy. Contractors should not appoint anyone without the prior approval of facility authority. It is essential to periodically audit the security performance of contractors. The temporary employee should be made aware of all relevant company policies and procedures on the first day of his assignment.
- Restrict the movement of vehicles within the plant as they can be used as a weapon. Ensure vehicular parking outside the processing area at a safe distance so that no suicide bomber can cause catastrophe. All commercial vehicles (tankers, box trailers, delivery trucks, etc.) should be inspected prior to entering the site. The driver's ID and/or license and other documentation should be verified before allowing entry to the site. Unannounced deliveries should not be accepted without first contacting the shipper or the carrier or using some other reasonable method to ensure the validity of the delivery.
- To thwart an intruder from forcing the operator to perform an unsafe operation of a critical valve, the operator should be able to, by the click of a switch, irreversibly disable the valve, transfer control to a centralised place and alert the security.

- Ban all personal items such as mobile phones, carry bags, extra clothing, purses, etc., in the process areas. Employee cafeteria and change rooms should be at an appropriate distance from the processing area.
- Establish an effective emergency response plan (ERP) which covers both intentional and unintentional incidents.
- Survey surrounding areas and look for activities that can affect the security of the facility, for example presence of high rise buildings, bridges, other likely targets, etc.
- If partial truck deliveries are being received and the truck has material for other plants too, then get your material at the end so the truck enters the premises with it and leaves empty. If it is not possible, then get your material delivered at the guardroom and then transfer it personally to the warehouse. This will avoid other unknown material from entering the premises.
- Similar precaution should be observed when dispatching material through hired trucks.
- In warehouse, if fire/explosion in one section will affect adversely the other sections due to shorter spacing between storages, consider fire walls/blast walls. Avoid glass window in warehouses through which incendiary material can be thrown in.

4.1.5. Training

Security awareness programme should be conducted for all employees and contractors, detailing terrorist information. They should be trained for specific skills like emergency response, bomb threats, hostage situation, first aid, etc. Encourage all employees and contractors to report the presence of unknown personnel, unidentified

vehicles, abandoned parcels or packages and any other suspicious activity within the plant. Security guards may be given specialised training for combating terrorist attacks. Drills form an essential part of the training and should be conducted under difficult conditions such as power outage, inclement weather conditions, etc. Managers should be trained to keep secret information intact and maintain good contact with the local law enforcement officials [2, 23].

4.2. Risk Management Strategies

Several risk management strategies, which are basically used for process safety, can also be utilised for improving security in CPI. Following risk management strategies are discussed here in brief, in view of process security:

- Inherently safer processes
- Rings of protection
- Incident reporting & investigation
- Management of change

4.2.1. Inherently Safer Processes (ISP)

The concept of inherent safety is based on the belief that if one can moderate or eliminate the hazard, not only the risk is reduced; it may be possible to remove it completely. In other words ISP would make hazard less likely to be realised and less intense if there is an incident. However, one should not forget the potential trade-offs that can occur while changing an approach or system. For example, chlorofluorocarbon (CFC) refrigerants are inherently safer with respect to fire/explosion and acute toxic hazards when compared to alternative refrigerants such as ammonia, propane, and sulphur dioxide. However, they are believed to cause long

term environmental damage due to stratospheric ozone depletion. Similarly, changing to a "just in time" inventory system could increase the number of shipments to a facility, thereby increasing the risk associated with transportation [32, 33, 34].

The best way to prevent terrorists attack is to reduce the attractiveness of the facility as a target. This objective can be achieved by utilising the concepts of ISP. The inherently safer process employs four key methods:

- Intensification
- Substitution
- Moderation
- Simplification

The principles of inherently safer processes are discussed here in the light of process security.

4.2.1.1. Intensification

This recommends the use of minimal amount of Hazchems in a process by introducing intensified designs for process equipment. Such equipment being smaller in size contains less amount of Hazchems, so a major crisis is not created even if the total equipment contents are lost. For example, short vertical towers contain less material and are less vulnerable than long vertical towers to projectiles, which may be fired at from outside the perimeter.

4.2.1.2. Substitution

It is important to substitute Hazchems with less hazardous ones wherever possible. For example: In Washington, D.C., the city's Blue Plains sewage treatment plant is switching from volatile chlorine gas to less volatile sodium hypochlorite bleach, which has far less potential for airborne off-site impact [35].

4.2.1.3. Simplification

In order to reduce the risk associated with toxic intermediates, alternative reaction routes should be considered. The reaction intermediate of insecticide, Carbaryl is methyl isocyanate, which created havoc at Bhopal in December 1984. After the Bhopal accident, DuPont Ltd. eliminated all storage of methyl isocyanate by switching to a closed loop process that only manufactures as much of the chemical as is required immediately in the process [35].

4.2.1.4. Moderation

Evaluate processing and storage of Hazchems under moderate conditions. For example, ammonia and chlorine can be stored at low pressure under refrigerated condition instead of at high pressure and ambient conditions. Even in case of intentional release of these chemicals, the evaporation rate would be comparatively small and is expected to cause less damage.

4.2.2. Rings of Protection

A concept of concentric rings of protection (Figure 4.2.2.1) that is similar to the concept of "Layers of Protection" of safety can be used in process security [11, 12]. This means that, if possible, the most important or most vulnerable assets should be placed in the centre of concentric levels of increasingly stringent security measures. For example, a chemical plant's electronic control room should not be placed right next to the building's reception area; rather, it should be located deeper within the building so that, to reach the control room, an intruder would have to penetrate numerous rings of protection, such as a fence at the property line, a locked exterior

door, an alert receptionist, an elevator with key controlled floor buttons, and a locked door to the control room.

In case of deliberate acts, the layers of protection must be particularly robust because adversaries will intentionally attempt to breach the protective measures.

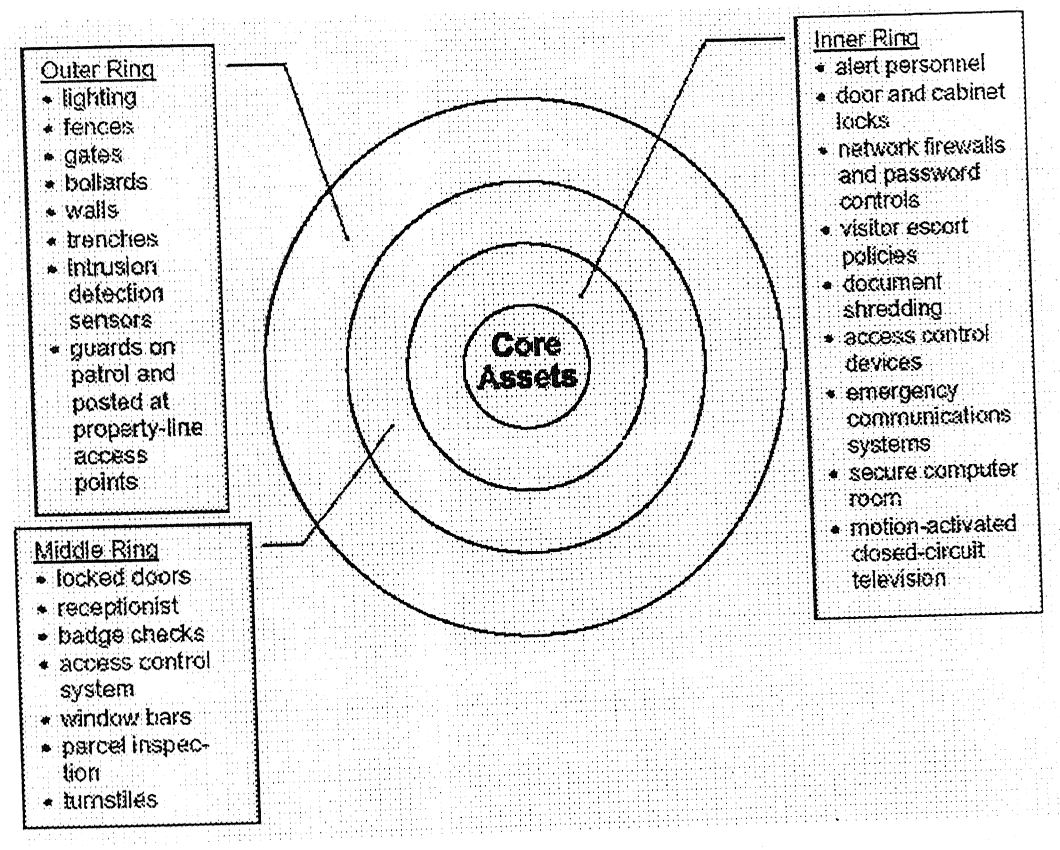


Figure 4.2.2.1. Rings of Protection [11]

4.2.3. Incident Reporting and Investigation

Incidents include suspicious events, breaches of the process security programme and actual attacks. Suspicious events may be a precursor to a well-planned attack. Such events should be properly reported and further investigated. Real attacks can be forestalled by the proper incident reporting and investigating [12, 30].

Any suspected illegal activity should be reported to law enforcement agencies. The following are some examples of security incidents that might warrant investigation:

- Unauthorised access by individuals in restricted areas
- Foreign vehicles in areas along the perimeter fencing, near buildings, security gates, etc.
- Individuals requesting information about the facility or company with no apparent need to know the information otherwise
- Unexplained loss of materials or product
- Cyber threats against control or computer systems
- Suspicious packages left at or suspect mail directed to the facility
- Doors or fences including gates not secured with indications of illegal entry

4.2.4. Management of Change

Conditions at process plants change constantly. Employees come and go; processes are modified, and threats wax and wane. This could lead to increased risk if the security management programme is not modified to accommodate the change. In process safety management this comes under Management of Change (MOC) that addresses the change that affects the process. This can be modified for managing security as well. It is important to address changes in following [12, 30]:

- New construction in and around the facility such as roads, new buildings, new equipment, etc.
- Employees and contractors
- Security devices, e.g. modifications to barriers, intrusion detection system, etc.
- Security procedures, e.g. access control, inventory control, ID cards
- Computer and information systems
- Threat levels
- Process conditions
- Growth of vegetation
- Any abnormal change in the behaviour of a employee/contractor and his life style
- Any significant change in a facility or operation such as a change in production quantities or methods, product type, shipping method, supplier, etc.
- Security-relevant personnel issues, such as transfers, suspensions, terminations, labour unrest, or employees exhibiting unusual behaviour
- Restarting equipment or systems that have been out of service for an extended time or that have not been maintained
- Changes in the environment of the plant for example, foliage growth, population growth, building development, etc.

Chapter 5

EMERGENCY RESPONSE

5.1. Emergency Response

The primary objectives of an effective emergency response plan (ERP) are safety of people, protection of property, and restoration of normal operation with minimum delay. Chemical plants have good safety and security regimes and access to them is generally restricted to authorised personnel only. These facilities are well designed to meet the abnormal events like technological malfunctioning and expected natural disasters, and access to these is restricted to the authorised personnel only. However, these were not designed in their inception, keeping in mind the risks from terrorist threats; and terrorists come up with unique ways of attack and give very little time for a response. Therefore, the chances for their success can not be ruled out [1, 2, 3].

In accidental ERP, a set of procedures have been developed over years; and it is mandatory for chemical plants handling large quantities of Hazchems to have an on-site contingency plan. On-site contingency plan is the primary responsibility of the facility whereas off-site emergency plan comes under local law enforcement.

Some important information that an accidental emergency plan should address include [36]:

- Roles and responsibilities of key persons in case of emergency.
- Identification of hazardous chemicals, processes and operations.
- Release scenarios, consequences in terms of heat radiation, over pressure and intoxication.
- Detailed site plan incorporating the damage contours.

- Identification of vulnerable zone.
- Detailed procedures for handling fire and other types of emergencies.
- Evacuation routes, assembly points, shelter in-place, first aid, etc.
- Requirements of various departments and organisations for coping with emergency situations, etc.

For accidental ERP, it is possible to anticipate most hazards and how to cope with them. However, it is very difficult to predict the events that can follow during and after terrorist attacks or other malicious acts. In such conditions establishing an emergency plan is not an easy task and cannot be accomplished by a single individual. It is essential that important functional groups such as safety, medical, security, and law enforcement provide the necessary inputs in preparing and executing an emergency plan. This would require modifications in existing ERP in light of intentional threats. The following points are important for ERP related to threats due to deliberate acts [1, 2, 37]:

- Inform local law-enforcement officials of terrorist activity or any other suspicious activities in the plant and areas surrounding it.
- Be careful in responding to the terrorists during attacks. There may be a delayed explosion from a "secondary device." Terrorists use a variety of distraction techniques such as small explosions to attract attention. Once security guards, employees, etc. have assembled, a larger, more powerful explosive may be detonated at a more critical site.
- All existing active and passive safeguards such as dikes, water sprinkler systems, foam systems, etc. will help in reducing the impact of attack. Ensure that these are in working conditions and not disabled by adversaries.

- Define evacuation procedures and shelter locations.
- Develop fire suppression, fire control, and system shut down procedures.
- Terrorists frequently strike multiple targets simultaneously. They may strike at one place to divert the attention and then attack other vital places. It is extremely important to maintain security intact at all vulnerable points during the attacks.
- Be prepared for possible attacks on emergency responders, rescue teams, etc. Maintain back up teams.
- Train emergency responders for disposing bombs and other anti-personnel devices.
- Train security personnel for safety procedures as well. They should be aware of the potential hazard in the facility and what should be done to prevent an accident.
- Provide power back-up for critical equipment and to carry out emergency plans.
- Develop communication systems that are not easily disabled during emergency. It is important to place communication wires in rigid conduits so that these can not be damaged easily.
- Establish procedures for dealing with public and media during attacks. With the co-operation of the media, the exact casualties and losses may not be announced immediately. This will deprive the terrorist of their satanic pleasure. It should however be ensured that public take appropriate precautions.
- Develop clear guidelines to work with outside organisations, i.e., fire fighters from various depots, police, army, media, medical team, law enforcement, etc.
- Conduct regular emergency drills in association with the local authorities and national organisations. Also, organise surprise drills in difficult conditions such as power outage, or inclement weather conditions. This exercise will provide the opportunity to have good co-ordination in various departments and organisations

involved in managing emergency. Include lessons learnt from such exercises in ERP. Mock terrorist drills are performed in nuclear power plants in various countries; the same can be followed in CPI handling bulk of Hazchems.

Chapter 6

CASE STUDIES

In this chapter two case studies have been performed: first on a fertiliser plant and the other on a refinery to show the application of ideas presented in the previous Chapters.

6.1. Case Study of a Fertiliser Plant

In this section, a case study has been performed on a fertiliser plant (X) to evaluate the security risks and recommendations are made to improve its site security.

6.1.1. Facility Description

Plant X produces ammonia using naphtha as the raw material. Ammonia is further converted to urea, the final product. Important site information, vital for risk assessment is as follows (Figure 6.1.1.1):

- Plant (X) is situated at a distance of 25 km from a major city on a national highway. The processing area is not visible from the national highway, but the naphtha storage tanks and other taller units can be seen from a side road.
- It produces 800 MTPD of ammonia and 1,400 MTPD of urea.
- Ammonia is stored in two large refrigerated (-34 °C) storage tanks (20 m diameter) of 7,500 MT capacity each.
- Naphtha is transported into site through rail cars and stored in tank farm consisting of 6 tanks (20 m diameter) of 5,000 MT capacity each.

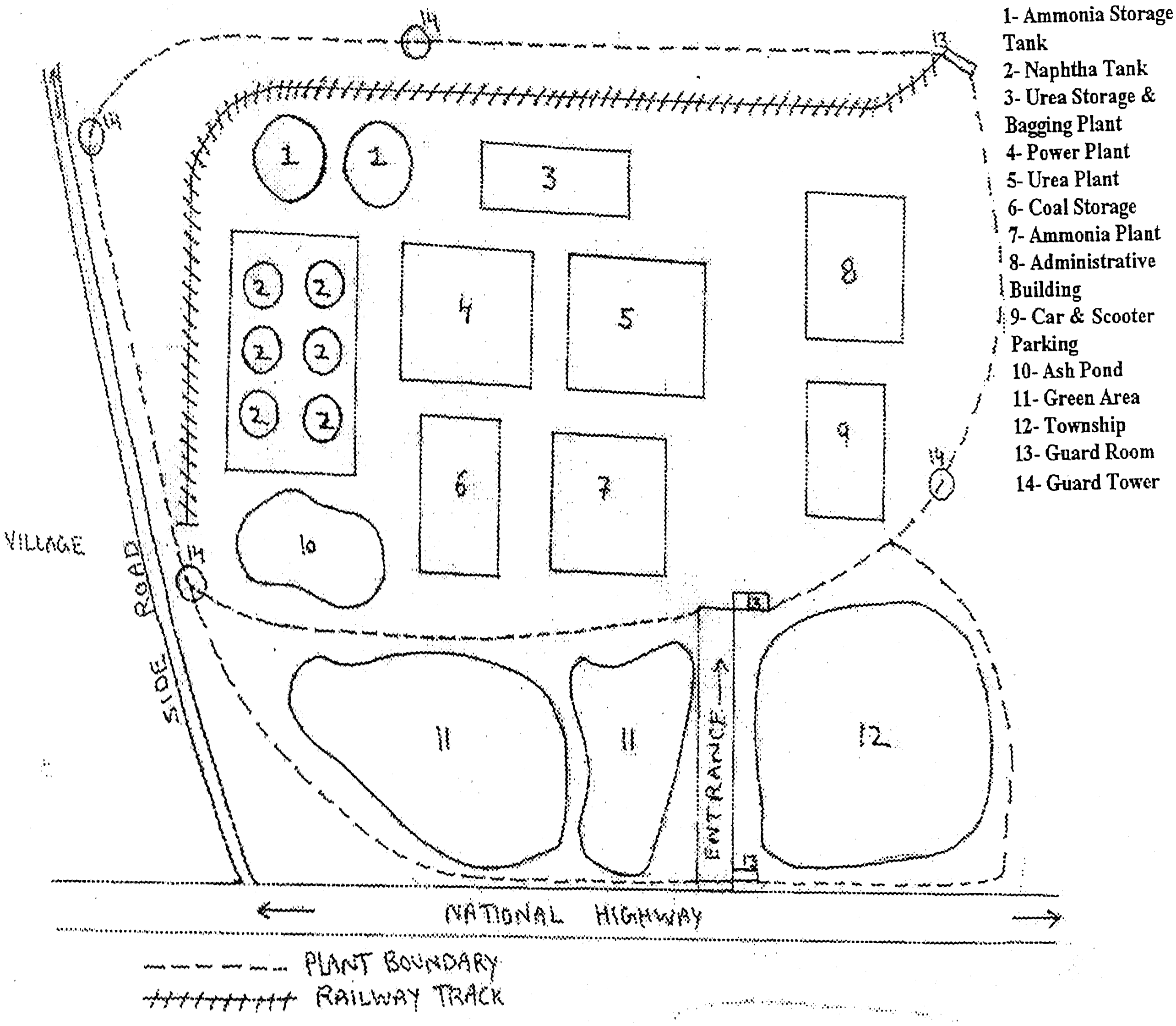


Figure 6.1.1.1. Sketch of Plant X

- Limited quantity of chlorine is stored in 8 cylinders (stored at ambient temperature, and at 788.1 kPa gauge pressure) of 1 tonne capacity each.
- Plant has a good safety record and is well prepared for dealing with any technical emergency. Guards are deployed for maintaining the security.
- The place has been free from terrorist activities in the past, but there have been a few minor security incidents in and around the facility.

6.1.2. Risk Assessment

Major Hazchems handled are naphtha, ammonia and chlorine. Naphtha is highly flammable, whereas ammonia and chlorine are highly toxic in nature. In the event of deliberate release of Hazchems, their impact can be estimated by consequence analysis. For ammonia and chlorine release, hazard distance (ERPG-2) is calculated using Dow's Chemical Exposure Index Guide [38].

If 5,000 tonne of ammonia is stored in one of the tanks and release takes place through a 25.4 cm diameter hole, located at the lower end of the shell, then the hazard distance for this scenario comes out as 4,492 m. Similarly, if chlorine is released through a 1.9 cm vapour connection of a cylinder, hazard distance will be 1,878 m. For tank farm containing naphtha, if pool fire is assumed in one of the tanks, the damage distance for heat radiation (12.5 kW/m^2) from the edge of the pool comes out as 32 m (See Appendix A for detailed calculations).

This shows that plant X will have serious off-site impacts in the event of deliberate release of Hazchems.

Threat Analysis

Types of threats: The following major threats are identified:

- Intentional release of ammonia and chlorine from storage tanks, cylinders and pipes.
- Fire and explosion in naphtha storage tanks.
- Fire and explosion in power generation and ammonia plant.
- Theft of ammonia for making bomb or illegal drug.
- Cyber attack through computer controlled equipment.
- Contamination of urea and naphtha.

Sources of threat: Terrorists (both domestic and international), disgruntled employees, contractors and criminals are taken as potential adversaries for plant X.

Vulnerability Analysis

VA is performed on plant X as described in Chapter 3. The plant is divided into different security zones as follows:

Zone 1: Low-risk areas such as green belt, unoccupied area, ash ponds, etc.

Zone 2: Moderate-risk areas such as product storage, offices, buildings, etc.

Zone 3: High-risk areas such as plant utilities, loading and unloading section, and pipe network containing ammonia, chlorine and naphtha.

Zone 4: Critical-risk areas such as naphtha and ammonia storage, equipment handling Hazchems, control room, etc.

Sample vulnerability assessment worksheet has been filled for ammonia storage tanks (Table 6.1.2.1) detailing threats, vulnerabilities, possible consequences and recommendations. This worksheet can similarly be completed for other assets of the plant.

Table 6.1.2.1. Vulnerability Assessment Work Sheet for Plant X
Critical area: Ammonia storage tanks

Threats	Vulnerabilities	Consequences	Recommendations
Ammonia release caused by terrorists.	1. Ammonia tanks are close to perimeter and labelled. 2. Vehicle movement near tanks is not controlled. 3. No guard patrol during daytime. 4. Projectiles could be fired or explosives charged.	Mass casualties both on- and off-site, environmental impact, financial loss and damage to company image.	1. Signage on ammonia tanks should not be visible from outside. 2. Install CCTV monitoring. 3. Make a permanent guard post near the tanks. 4. Consider installing projectile shield.
Ammonia release caused by a disgruntled employee.	1. Employee access to this area is not controlled. 2. Drain valve can be opened manually. 3. Poor labour relations.	Injuries on-site, environmental impact, loss of confidence in employees and damage to company image.	1. Restrict access of employees to this area. 2. Consider installing valve locks. 3. Maintain good labour relations.

Security Risk Factor Table (SRFT)

SRFT has been completed for plant X. The total score obtained in SRFT suggests that it is a high-risk facility (Table 6.1.2.2). Based on the outcome of the security risk assessment of plant X, following recommendations are made.

Recommendations

- Ban mobile phones and other electronic devices in processing area.
- Move car/scooter parking out of processing area.
- Remove vegetation in and around naphtha and ammonia storage area, so suspicious activities can easily be monitored and they will not sustain any fire.
- Ensure proper access control in plant; restrict employee access to zone 4.
- Do not use the naphtha tanks located towards the plant boundary or store less amount of in it.
- Ensure vehicle barricades and a permanent guard post near ammonia tanks.
- Provide valve locks at important locations.
- Install CCTV in naphtha tank farm area and near ammonia tanks.
- Regularly inspect the rail cars for explosives that carry naphtha to the plant.
- Avoid signage on ammonia and naphtha tanks.
- Install pointed sprays (water, mace, etc.) to surprise a suspicious person attempting to enter at the guardroom. This gives time for security personnel to act.
- Install guard towers around the perimeter that there are no dead spots. Consider equipping guard towers with night vision devices.
- Maintain good labour relations in the plant.
- Maintain good contacts with the law enforcement officials.

Table 6.1.2.2. Security Risk Factor Table for Plant X

Risk factors	**Range of security points**				**Actual points**
Location	Rural 1	Urban 2,3,4		High density 5	1
Visibility	Not visible 0	Low 1,2	Medium 3,4	High 5	2
Inventory	Low 1	Medium 2	Large 3,4	Very large 5	5
Ownership	Private 1	Public/Co-operative 2,3		Government 4,5	3
Presence of chemicals which can be used as precursor for WMD	Absence 0			Presence 5	0
Worst case impact on-site	Negligible 0	Low 1	Moderate 2,3,4	Severe 5	5
Worst case impact off-site	Negligible 0	Low 1	Moderate 2,3,4	Severe 5	4

Contd…

Table 6.1.2.2. Security Risk Factor Table for Plant X (Contd…)

Risk factors	Range of security points			Actual points
History of security incidents	Nil 0	Few 1,2,3	Frequent 4,5	2
Presence of terrorist groups in region	Absence 0	Few 1,2,3	Large no. 4,5	0
Existing security measures:	High level	Ordinary	Poor / None	
• Access control	1	2,3	4,5	3
• Perimeter protection	1	2,3	4,5	2
• Mitigation potential	1	2,3	4,5	1
• Proper lighting (all over)	1	2,3	4,5	2
• Use of Metal detector/ x-ray/ CCTV (at entrance and at all critical locations)	1	2,3	4,5	3
Personal preparedness and training	Well prepared 1	Average 2,3	Poor 4,5	2
				Total score = 35

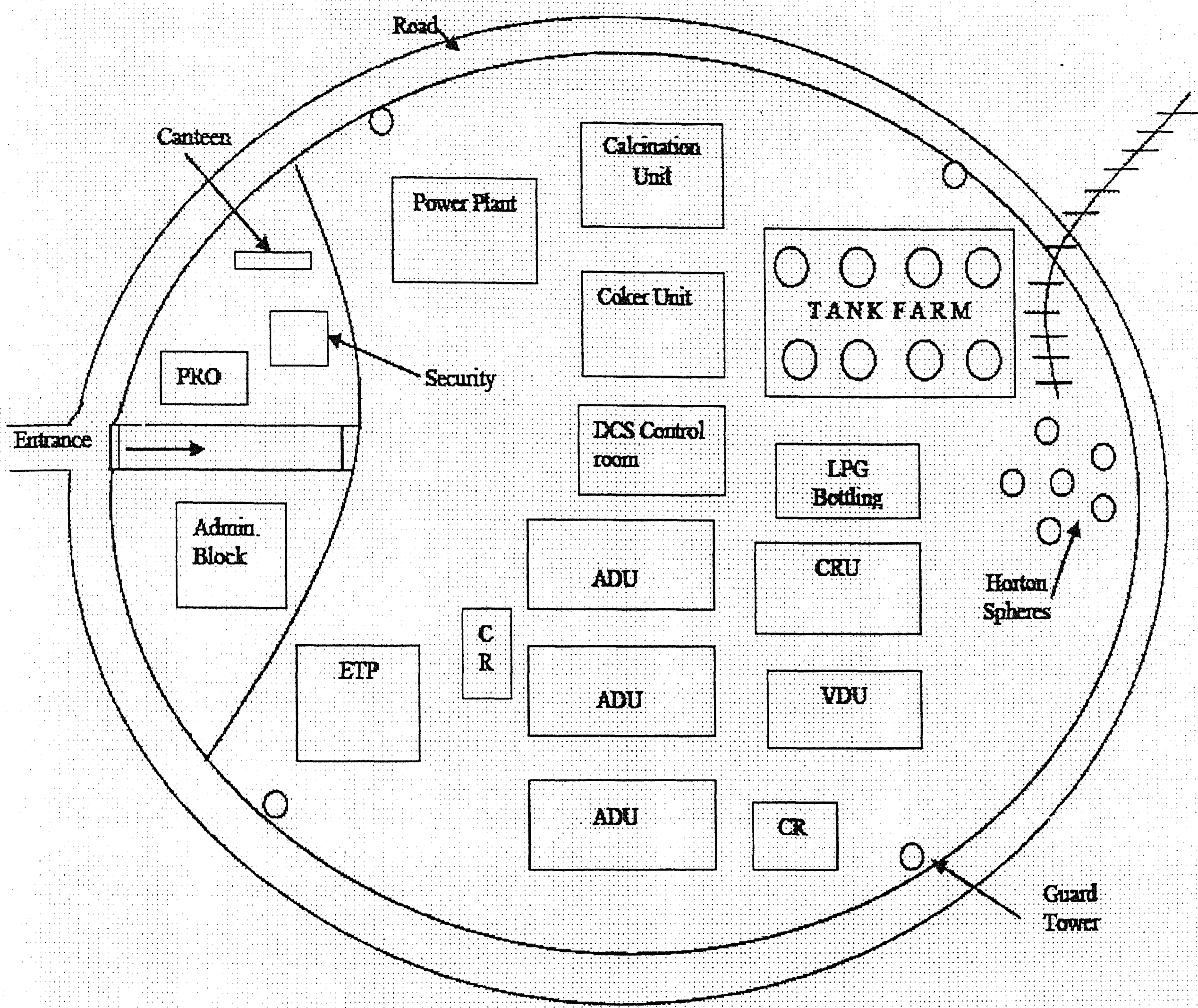
6.2. Case Study of a Refinery

In this section, a refinery (Y) is considered as a possible target for terrorist attacks. Risk assessment techniques as described in Chapter 3 are applied to evaluate the security risks and important recommendations are made to improve its site security.

6.2.1. Facility Description

Refinery Y is involved in producing all major petroleum products. Crude oil comes to the refinery via pipeline and final products are sent out through pipelines as well as by road tankers and rail wagons to the marketing terminals. Important site information, vital for risk assessment, is as follows (Figure 6.2.1.1):

- It is situated in a remote location and the nearest city is 20 km away. There are four small villages that surround the site and the refinery township is 1 km away from the refinery.
- The processing area is not visible from the main highway, but the storage tanks and other taller units can be seen from some parts of the road that surrounds the perimeter.
- Various petroleum products, both crude and finished, are stored in different storage tanks in a tank farm area. Crude oil is transported into site through rail cars and pipelines. Final products are dispatched to various marketing terminals by rail wagons, road tankers and by pipelines.
- Refinery has its own power generation plant, effluent treatment plant, and township for its employees.
- It has a good safety record and is well prepared for dealing with any technical emergency.



ADU = Atmospheric distillation unit
VDU = Vacuum distillation unit
CRU = Catalytic reforming unit
CR = Control room
PRO = Public relation office
ETP = Effluent treatment plant

Figure 6.2.1.1. Sketch of Refinery Y

- Several units of paramilitary forces are deployed for maintaining the security. The use of security equipment such as CCTV, explosive and metal detectors are limited, and access control procedures followed are average.
- There have been a few unsuccessful attempts of blowing up the pipeline in the past in the region. A few cases of theft and violence have been reported in and around the facility.

6.2.2. Risk Assessment

Majority of chemicals handled at refinery Y are highly flammable and pose fire and explosion hazards.

Threat Analysis

Types of threats: The following major threats are identified:

- Intentional release of petroleum products from storage tanks and pipelines.
- Serious disruption in production by changing settings at the control rooms.
- Fire and explosion in atmospheric vacuum distillation unit, power generation and catalytic reforming unit.
- Possible cyber attack through computers attached to the control systems.
- Fire and explosion in loading and unloading sections.
- Contamination of raw material or finished product.

Sources of threat: All sources of threats as outlined in Table 3.1.1 are considered possible adversaries for refinery Y.

Vulnerability Analysis

Vulnerability analysis can be performed on refinery Y as described in Chapter 3. Refinery Y is divided into various security zones as follows:

Zone 1: Low risk areas such as green belt, unoccupied area, effluent pond, etc.

Zone 2: Moderate risk areas such as plant utilities, offices and buildings, etc.

Zone 3: High-risk areas such as loading and unloading sections, power generation unit, pipelines carrying flammable material, etc.

Zone 4: Critical risk areas such as tank farm, horton spheres, atmospheric vacuum distillation unit, LPG bottling plant, catalytic reforming unit, control rooms, etc.

Consider a particular critical risk area such as tank farm or control room. Sample vulnerability assessment worksheet has been filled up for these areas detailing threats, vulnerabilities, possible consequences and recommendations (Tables 6.2.2.1 & 6.2.2.2). This work sheet can similarly be developed for any other specific area of the refinery.

Table 6.2.2.1. Vulnerability Assessment Work Sheet for Refinery Y
Critical area: Tank farm

Threats	Vulnerabilities	Consequences	Recommendations
Fire and explosion caused by terrorists.	1. Some storage tanks are close to perimeter and labelled. 2. Vehicle movement near tanks farm is not controlled. 3. No guard patrol during daytime.	Casualties both on- and off-site, environmental impact, severe financial loss and damage to company image.	1. Avoid signage on storage tanks mentioning quantity and material stored. 2. Install CCTV monitoring. Provide vehicle barrier near tank farm. 3. Provide around the clock guard post near tank farm.
Fire and explosion caused by disgruntled employees.	1. Employee access to this area is not controlled. 2. Drain valve can be opened manually. 3. Poor labour relations.	Injuries on-site, environmental impact, loss of confidence in employees and damage to company image.	1. Restrict access of employees to this area. 2. Consider installing valve locks. 3. Maintain good labour relations in the refinery.

Security Risk Factor Table (SRFT)

SRFT has been completed for refinery Y. The total score obtained in SRFT suggests that it is a high-risk facility (Table 6.2.2.3).

Recommendations

Since refinery Y is a high-security risk facility, so most of the recommendations for improvement are similar to that of fertiliser plant X. Recommendations for refinery Y are:

- Ban cigarettes, match sticks, cigarette lighter, mobile phones and other electronic devices in refinery.
- Provide car parking out of the processing area.
- Ensure proper access control in refinery; restrict employee access to Zone 4; permit only authorised people.
- Do not use storage tanks located very close to the plant boundary to store hazardous/flammable chemicals; use them for emergency purposes only.
- Ensure vehicle barricades near catalytic reforming unit, atmospheric vacuum distillation unit.
- Install CCTV surveillance in Zone 4 and other areas where regular patrol is not feasible.
- Regularly inspect for explosives the rail cars and road tankers that carry crude oil to the refinery or products out of.
- Avoid signage on vessels and storage tanks mentioning quantity and type of material handled.
- Frequently alter protocol for flammable material storage to increase its security.

- Install pointed sprays (water, mace, etc.) to surprise a suspicious person attempting to enter at the guardroom. This gives precious time for security personnel to act.
- Install guard towers around the perimeter such that there are no dead spots. Equip guard towers with searchlights, night vision devices, and multiple communication channels to the security control room.
- Maintain good contacts with the law enforcement officials, neighbouring communities, and other plants.

Table 6.2.2.3. Security Risk Factor Table for Refinery Y

Risk factors	**Range of security points**				**Actual points**
Location	Rural 1	Urban 2,3,4		High density 5	1
Visibility	Not visible 0	Low 1,2	Medium 3,4	High 5	1
Inventory	Low 1	Medium 2	Large 3,4	Very large 5	5
Ownership	Private 1	Public/Co-operative 2,3		Government 4,5	5
Presence of chemicals which can be used as precursor for WMD	Absence 0			Presence 5	0
Worst case impact on-site	Negligible 0	Low 1	Moderate 2,3,4	Severe 5	5
Worst case impact off-site	Negligible 0	Low 1	Moderate 2,3,4	Severe 5	3

Contd...

Table 6.2.2.3. Security Risk Factor Table for Refinery Y (Contd…)

Risk factors	**Range of security points**			**Actual points**
History of security incidents	Nil 0	Few 1,2,3	Frequent 4,5	3
Presence of terrorist groups in region	Absence 0	Few 1,2,3	Large no. 4,5	3
Existing security measures:	High level	Ordinary	Poor / None	
• Access control	1	2,3	4,5	2
• Perimeter protection	1	2,3	4,5	2
• Mitigation potential	1	2,3	4,5	2
• Proper lighting (all over)	1	2,3	4,5	3
• Use of Metal detector/ x-ray/ CCTV (at entrance and at all critical locations)	1	2,3	4,5	3
Personal preparedness and training	Well prepared 1	Average 2,3	Poor 4,5	2
				Total score = 40

Chapter 7

CONCLUSIONS
AND
RECOMMENDATIONS FOR FUTURE WORK

7.1 Conclusions

Terrorists often attack less protected targets such as public mall, railway stations, and other crowded locations where they can inflict maximum damage by using conventional weapons. They may not prefer attacking chemical plants for two reasons. First, it is difficult to intrude into these facilities and chances of their success are not high. Second, these plants are mostly well equipped for meeting emergencies. However, these plants were not designed keeping in mind the risks from terrorists, and consequences in case of a successful attack may be enormous. Therefore, the threats from deliberate acts are real and require chemical facilities to implement appropriate site security guidelines.

This work has identified some of the threat sources, types, and threat scenarios that a plant may experience. Security risk assessment is carried out qualitatively by conducting threat and vulnerability analysis, and developing Security Risk Factor Table. Various security countermeasures are suggested to improve security of chemical plants. However, it is not recommended to turn chemical facilities into a fort or resemble a defence installation. For highly motivated terrorists, facilities with high security sometimes become an attractive target as they may take it as a challenge to breach the security of such facilities to show their strength.

The conventional safety and security measures that were in place before 9/11 will also serve well for deliberate acts. Many of the safeguards such as excess flow valves, pressure relief systems, systems to interrupt run away reactions, and other safety equipment will reduce the consequences during terrorist attacks as well. Terrorism and sabotage may be taken as an initiator cause for HAZOP or other safety tools. Idea is to apply the existing safety tools to deliberate acts. Innovative thinking is required to reduce the target attractiveness, and implement effective countermeasures that may provide an element of surprise to the adversaries.

There is a need to have a balance on safety and security aspect of information. While confidential information about the facility may not be revealed to the surrounding community, they must be made aware of the general hazards and emergency procedures. They will come to help in case of a terrorist attack.

Security is a dynamic issue and terrorists employ some unthinkable and unseen measures in planning attacks. It is extremely important to reduce the attractiveness of chemical plants as target and what should be done to reduce the consequences in case of successful attacks. Besides safety and environmental considerations, security risks should be evaluated while deciding on location and layout of new plants. There should be some legislation requiring operators to maintain a certain standard of security in chemical plants.

To sum up, while CPI must take terrorists act into account in planning security and emergency management plans, there does not seem to be a need to be unduly concerned because a lot of safety and emergency handling procedures have been put in place especially since the Bhopal Gas Tragedy of 1984.

7.2. Recommendations for Future Work

In the present work, security risk assessment of CPI has been conducted qualitatively by threat and vulnerability analysis, and developing Security Risk Factor Table. The work also addressed some effective security countermeasures and risk management strategies that would help CPI to deal with deliberate threats. However, the research work in the field of security is in the starting phase so there are several things that can be tried in future. Some of the recommendations for future work are:

- Some quantitative risk assessment methods should be developed for addressing the risks from deliberate acts. Loss event profile, probability and criticality are important in quantifying security threats.
- Existing accidental safety tools such as fault tree, event tree, what-if, checklist, etc., can be developed for the deliberate acts.
- HAZOP type software can be made for assessing the vulnerabilities of CPI.
- Research is required to study the response of a process for intentional acts and what should be done to minimise the impact of successful attack.
- Research is required to improve the physical and cyber security of CPI.
- Some standard for observing physical and cyber security in CPI should be developed.
- Process vessels and storage tanks can be designed to withstand terrorist attacks.
- Process control systems can be designed such that ill-willed insiders can not create destructive situations by disturbing control settings.

References

1. S. Bajpai and J. P. Gupta, *Protecting Chemical Plants from Terrorist Attacks*, Chemical Weekly, 2005, Vol. L (34), 209-213.

2. S. Bajpai and J. P. Gupta, *Site Security for Process Industries*, presented in International Conference on Bhopal Gas Tragedy and its effects on Process Safety, December 1-3, 2004, Indian Institute of Technology, Kanpur, available at: http://www.iitk.ac.in/che/jpg/papersb/full%20papers/B-126.doc

3. S. Bajpai and J. P. Gupta, *Securing Oil Infrastructure*, presented in Kuwait Oil and Gas Conference and Exhibition, March 7-9, 2005, Kuwait city, Kuwait.

4. American Petroleum Institute, *Security Guidelines for the Petroleum Industry*, 2003, Washington DC, available at: http:// www.api-ec.api.org/filelibrary/Security_Guidance2003.pdf

5. http://news.bbc.co.uk/go/pr/fr/-/2/hi/asia-pacific/4365417.stm

6. P. Baybutt, *Process Security Management: Set Up Your Plant's Program*, Chemical Engineering, 2003, Vol. 110(1), 48-56.

7. www.chemalliance.org/docs/SECALE-F.PDF

8. http://www.acusafe.com/Newsletter/Stories/1001News-MonthlyIncidents.htm

9. http://www.nrdc.org/media/pressreleases/030909.asp

10. C. A. Ropar, *Risk Management for Security Professionals*, Butterworth Heinemann, 1999, New Delhi.

11. American Chemistry Council, Chlorine Institute, and Synthetic Organic Chemical Manufacturers Association, *Site Security Guidelines for the US Chemical Industry*, 2001, Washington DC, available at: http://www.accnewsmedia.com/docs/100/89.pdf

12. Center for Chemical process Safety, *Guidelines for Analyzing and Managing the Security Vulnerabilities of fixed Chemical Sites*, 2003, New York.

13. Synthetic Organic Chemical Manufacturers Association, *Manual on Chemical Site Security Vulnerability Analysis Methodology and Model SVA*, 2002, Washington DC.

14. American Petroleum Institute, *Security Vulnerability Assessment Methodology for the Petroleum and Petrochemical Industries*, Second Edition, 2004, Washington DC.

15. P. Baybutt, *Assessing Risks from Threats to Process Plants: Threats and Vulnerability Analysis*, Process Safety Progress, 2002, Vol. 4, 269-275.

16. P. Baybutt, *Inherent Security: Protecting Process Plants Against Threats*, Chemical Engineering Progress, 2003, 35-38.

17. J. R. Lemley, V. M. Fthenakis, and P.D. Moskowitz, *Security Risk Analysis for Chemical Process Facilities*, Process Safety Progress, 2003, Vol. 22 (3), 153-162.

18. C. D. Jaeger, *Chemical Facility Vulnerability Assessment Project*, Journal of Hazardous Materials, 2003, Vol. 104(1-3), 207-213.

19. D. A. Moore, *The New Risk Paradigm for Chemical Process Security and Safety*, Journal of Hazardous Materials, 2004, Vol. 115, 175-180.

20. R. P. Stickles, H. Ozog and S. Mohindra, *Security Vulnerability Assessment (SVA) Revealed*, white paper of ioMosaic Corporation, 2003, Salem, available at: http://www.archives1.iomosaic.com/whitepapers/SVA.pdf

21. M. N. Coster and R. K. S. Hankin, *Risk Assessment of Antagonistic Hazards*, Journal of Loss prevention in Process Industries, 2003, Vol. 16(6), 545-550.

22. S. D. Emerson & J. Nadeau, *A Coastal Perspective on Security*, Journal of Hazardous Materials, 2003, Vol. 104, 1-13.

23. P. T. Ragan, M. E. Kilburn, S. H. Roberts & N. A. Kimmerle, *Chemical Plant Safety: Applying the Tools of the trade to a New Risk*, Chemical Engineering Progress, February 2002, 62-68, available at: http://www.cepmagazine.org/pdf/020262.pdf

24. J. R. R. Whiteley and M. Sam Mannan, *Initial Perspectives on Process Threat Management*, Journal of Hazardous Materials, 2004, Vol. 115, 163-167.

25. D. Teumim, *Are Your Plants and Pipelines Safe from Cyber Attack?*, Chemical Engineering Progress, 2002, 69-73.

26. P. Baybutt & V. Reddy, *Strategies for Protecting Process Plants against Terrorism, Sabotage and other Criminal Acts*, Homeland Defence Journal, 2003, Vol. 2, 1.

27. http://www.chemical-safety.com/documents/pdf/SECURITY%20RAT.pdf

28. http://primatech.com/info/paper_the_business_case_for_cyber_security.pdf

29. D. L. Berger, *Industrial Security*, second edition, Butterworth Heinemann, 1999, New Delhi.

30. American Chemistry Council, *Implementation Guide for Responsible Care Security Code of Management Practice, Site Security & Verifications*, 2002, Washington DC, available at, http://www.americanchemistry.com/rc.nsf/2febeebd340dda4a8525680b004b7f4a/67f8d93b3af1da8685256ccd005946c8/$FILE/Responsible%20Care%20Site%20Security%20Guidance.pdf

31. J. J. Fay, *Contemporary Security Management*, Butterworth Heinemann, 2002, New Delhi.

32. D.C. Hendershot, *Inherently safer chemical process design*, Journal of Loss Prevention in Process Industries, 1997, Vol. 10(3), 151-157.

33. J. P. Gupta, *A course on Inherently Safer Design*, Journal of Loss Prevention in Process Industries, 2000, Vol. 13, 63-66.

34. T. Kletz, *Process plants: A handbook for inherently safer Design*, Taylor & Francis, 1998, Philadelphia.

35. http:// www.ems.org/chemical_plants/inherent_safety.html

36. B. V. Ramabrahman, *Model Off-Site Emergency Plan for Chemical Process Industries*, Seminar Proceeding of Industrial Safety, Hazard, and Risk Assessment, 16-17 November, 2003, National Productivity Council, Chennai, B-8/1-11.

37. S. Phong, *Disaster Preparedness Planning*, Safety and Loss Prevention in Chemical & Oil Processing Industries, Hemisphere Publishing Corporation, London, 1989, 42-48.

38. Dow Chemical Company, *Dow's Chemical Exposure Index Guide*, 1993, New York.

39. J. P. Gupta, *Short Course on Quantitative Risk Assessment and Hazard Analysis in Chemical Industry*, 1996, Indian Institute of Technology, Kanpur.

Appendix A

Consequence Analysis of Fertiliser Plant X

A.1 Liquid Ammonia Release Scenario (38)

Liquid ammonia release takes place through a 25.4 cm diameter hole, located at the lower end of the shell.

Needed information:

Density of liquid ammonia (-34°C), ρ	$= 682$ kg/m^3
Gauge pressure, P_g	$= 0$ kPa
Characteristic pool temperature, T	$= -34$°C
Height of liquid above the release point, Δh	$= 22.5$ m
Molecular weight, MW	$= 17$
Vapour pressure at characteristic pool temperature, P_V	$= 101.3$ kPa
$ERPG-2$ value for ammonia	$= 139$ mg/m^3

For 25.4 cm diameter hole, cross sectional area = 506.7 cm^2

Effective area, A = .20(506.7) cm^2

Effective hole diameter, $D = \sqrt{\frac{4}{\pi}A} = 11.35$ cm $= 113.5$ mm

Estimating liquid released

Liquid Release Rate, L = $9.44\times10^{-7} D^2 \rho \sqrt{\frac{1000P_g}{\rho} + 9.8\Delta h}$ kg/s ....(A1)

(Where D is in mm)

$$L = 9.44\times10^{-7}(113.5)^2(682)\sqrt{\frac{1000(0)}{682\rho} + 9.8(22.5)} \quad \text{kg/s}$$

= 124.21 kg/s

Estimating pool size

Total mass of the liquid entering the pool, W_P kg = Total liquid released, W_T kg

(Assuming, none of the liquid flashes)

W_P = 900 L = 900 (124.21) ....(A2)

= 111,794 kg

Pool area, $A_P = 100 \frac{W_P}{\rho}$ ....(A3)

= 16,394 m^2

Determining the airborne quantity evaporated from the pool surface

Air borne quantity from pool, $AQ_P = 9.0\times10^{-4}(A_P^{.95})\frac{(MW)P_V}{T+273}$ kg/s ....(A4)

$$= 9.0\times10^{-4}(15,457^{.95})\frac{(17)101.3}{-34+273} \text{ kg/s}$$

= 65.384 kg/s

Total air borne quantity, $AQ = AQ_P$ = 65.384 kg/s

Hazard distance, HD = $6551\sqrt{\dfrac{AQ}{ERPG-2}}$ m ....(A5)

= 4492 m

A.2 Chlorine Vapour Release

Chlorine vapour release takes place through a 1.9 cm vapour connection of a cylinder. The hazard distance for this scenario comes out as 1,878 m. (Please refer to Appendix 3 of Dow's Chemical Exposure Index Guide [38] for detailed calculations.)

A.3 Pool Fire in Naphtha Tank

If pool fire is assumed in one of the naphtha tank in tank farm, damage distance can be calculated as follows:

Damage distance for a given incident heat flux from the flame center [39]

$$= 1.079\left(\frac{E_P}{Q_i}\right)^{0.57} R_P \qquad \text{.............(A6)}$$

where,

E_P = Effective emissive power = 135 kW/m^2

Q_i = Incident heat flux = 12.5 kW/m^2

R_P = Pool radius = 10 m

From equation (A6),

Damage distance (12.5 kW/m^2 heat intensity) from flame center = 41.88 m

Damage distance (12.5 kW/m^2 heat intensity) from the edge of the pool = 31.88 m